计算机科学
COMPUTER SCIENCE

深度学习驱动下IaaS云运维异常检测算法的研究进展

司佳, 梁建峰, 谢硕, 邓英俊

引用本文

司佳, 梁建峰, 谢硕, 邓英俊. 深度学习驱动下IaaS云运维异常检测算法的研究进展[J]. 计算机科学, 2024, 51(6A): 230400016-8.

SI Jia, LIANG Jianfeng, XIE Shuo, DENG Yingjun. Research Progress of Anomaly Detection in IaaS Cloud Operation Driven by Deep Learning [J]. Computer Science, 2024, 51(6A): 230400016-8.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.230400016

深度学习驱动下 IaaS 云运维异常检测算法的研究进展

司　佳[1]　梁建峰[1]　谢　硕[1]　邓英俊[2]
1 国家海洋信息中心　天津 300171
2 天津大学应用数学中心　天津 300072
(sijia@nmdis.org.cn)

摘　要　异常检测是 IaaS 云系统运维中的一个关键任务,通过早期预警和提前干预,可有效避免系统崩溃等严重事故的发生。但相较于传统数据中心,IaaS 云系统具有较大规模的计算节点,节点拓扑复杂、监测数据量大、缺少标注信息等特点,为 IaaS 云运维异常检测带来新的挑战。从深度学习的技术框架出发,分析了异常检测问题面临的难点,调研总结了 IaaS 云系统下常见异常检测算法和相关技术。面向节点异常和系统异常两类典型问题,对深度学习驱动的解决方法进行调研:面向节点级别异常,重点调研了时间依赖的运维数据下由时序数据驱动的检测算法;面向系统级别异常,重点调研了网络拓扑建模下由图数据驱动的检测算法。最后,提出了数据驱动下 IaaS 云运维数据异常检测中的新问题与新挑战。

关键词:异常检测;IaaS 云平台;时序数据;图数据;深度学习;机器学习
中图分类号　TP311.1

Research Progress of Anomaly Detection in IaaS Cloud Operation Driven by Deep Learning

SI Jia[1], LIANG Jianfeng[1], XIE Shuo[1] and DENG Yingjun[2]
1 National Marine Data and Information Service, Tianjin 300171, China
2 Center for Applied Mathematics, Tianjin University, Tianjin 300072, China

Abstract　Anomaly detection is an important task in the operation and maintenance of IaaS cloud systems. Through early warning and intervention, serious accidents such as system crashes can be effectively avoided. However, compared to traditional data centers, IaaS cloud systemshave the characteristics of large-scale computing nodes, complex node topology, large monitoring data volume, and lack of data labels, which bring new challenges for IaaS cloud anomaly detection. Starting from the technical framework of deep learning, this paper analyzes the difficulties faced by anomaly detection problems, and summarizes common anomaly detection algorithms and related technologies in IaaS cloud systems. This paper investigates deep learning driven solutions for two typical problems: node anomalies and system anomalies. For node anomalies, detection algorithms driven by temporal data are studied for time-dependent data. For system anomalies, detection algorithms driven by graph data in network topology modeling are investigated. Finally, new issues and challenges in data-driven anomaly detection in IaaS cloud systems are proposed.

Keywords　Anomaly detection, IaaS cloud, Time series data, Graph data, Deep learning, Machine learning

1　引言

云计算是一种基于网络将计算资源、存储资源和网络资源集中到“云”端的计算范式,可实现资源的按需配置,向用户提供个性化服务,逐渐被关注和应用。随着云技术的迅速发展,越来越多的系统迁移上云[1-2],云平台的规模和复杂度持续增加。大规模、虚拟化、高共享等特点,使得云平台在运行中发生故障是不可避免的,这将影响到用户体验,造成经济损失,降低用户对云平台的信任。为了保证云平台运行的可靠性和安全性,针对云平台进行快速、精准、实时的异常检测,对于已出现或者可能出现的异常状况向运维人员提出告警,是重要且具有挑战的工作。云平台的异常检测问题已得到了广泛的关注,研究人员对运维监控数据进行分析,开发了各种各样的模型用于运维中的异常检测。本文深入调研 IaaS 云运维相关论文,分析 IaaS 架构下云运维中异常检测面临的问题,针对时序运维数据的时间相关性和云结构的空间相关性,将异常检测模型分为基于时序数据和基于图数据两类进行综述。

本文中深度学习驱动下异常检测算法的分类如图 1 所示。

基金项目:国家海洋信息中心青年基金项目(202102006);南海海洋资源利用国家重点实验室开放基金(MRUKF2021035)
This work was supported by the National Marine Data and Information Service Youth Fund Project(202102006) and Open Fund of State Key Laboratory of Marine Resources Utilization in South China Sea(MRUKF2021035).
通信作者:邓英俊(yingjun.deng@tju.edu.cn)

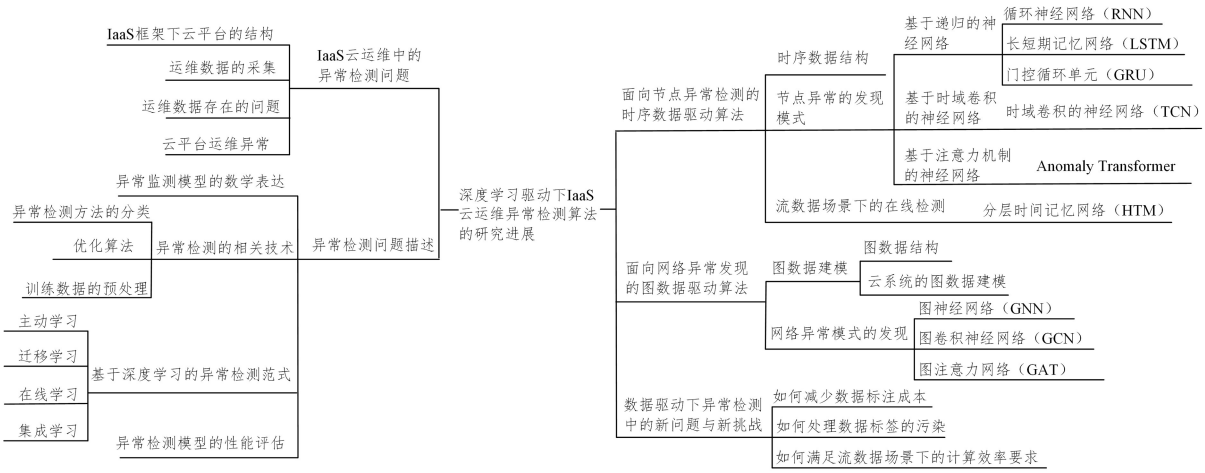

图 1 本文中异常检测算法的分类

Fig. 1 Classification of anomaly detection algorithms

2 IaaS 云运维中的异常检测问题

本章将重点分析 IaaS 架构下云平台的结构、异常检测的对象和面临的挑战。

2.1 IaaS 框架下的云平台结构

IaaS 框架下的云平台通过网络为用户提供计算资源、存储资源、网络资源等基础设施服务，通过虚拟化技术将所有资源整合为一个整体对外提供服务，包括硬件、软件、操作系统、存储等。IaaS 框架下的云平台将服务器、存储等设备划分为多个集群，通过虚拟化技术构成资源池，共同提供服务。在计算资源池中，物理服务器可虚拟化出多个虚拟机实例，它们共享 CPU、内存、硬盘等硬件资源。IaaS 云平台支持将运行的虚拟机快速地在服务器之间移动、复制和重新分配。云平台的灵活性使得虚拟机按照客户的需求创建，并且可以随时租用或削减资源，调整虚拟机配置。但灵活复杂的结构造成云计算中心出现故障的频率和可能性比传统的数据中心更高。

2.2 运维数据的采集

IaaS 云平台通过对基础设施、系统服务等的监控，为运维人员提供日常维护和维修保障的依据。运维监控目标一般包括硬件、系统、应用、网络、流量、日志、安全、API、性能、业务等多个方面。目前云平台运维相关研究工作主要依托 3 类数据进行，分别是性能指标[3-4]、日志[5]和请求追踪信息[6]。性能指标大多以时间序列指标的形式采集，通过轮询 IT 资源来收集云平台的运行数据，以周期性地监控 IT 资源状态。日志数据用于描述离散事件，例如运维人员的操作、云管理平台的动作、系统出错时的相关信息等等。第三类数据为请求追踪信息，用于追踪单次事务或者服务请求的处理情况。研究人员根据不同的数据类型构建了不同的异常检测模型。其中，性能指标包括云平台计算资源、存储资源、磁盘资源、进程信息、网络资源等监控数据，可通过分析其分布规律刻画数据中心的运行情况。本文关注于云平台性能指标的异常检测问题。

为推动云运维领域的研究，一些公司提供了数据集帮助研究者分析真实场景下异常检测所面临的问题与挑战，测试与比较不同算法的性能。NAB 数据集(The Numenta Anomaly Benchmark，NAB)[7]是一个流异常检测数据集，包含 58 个带有标注的真实数据和人工生成文件。NAB 同时提供一种异常检测的评分机制，并更新基于数据集和评分机制的算法排名。雅虎 Webscope 数据集由带有标记异常点的时序数据权成，包含从雅虎云平台中真实采集的数据以及人工合成的数据。清华大学公布了 3 个大规模真实数据集[8]，数据来自搜狗、易贝、腾讯等大型互联网公司，用于测试运维的异常检测、根因定位、故障发现与诊断等领域；并举办了三届智慧运维算法大赛。

2.3 运维数据存在的问题

1)数据量大。云监控系统为运维人员提供海量监控指标，形成时间序列形式的数据来表征云系统的运行状态。数量巨大、种类繁多的指标和高频率的刷新，造成运维数据量极为庞大。

2)召回率低[9]。在云系统的运行中，正常的运行占据绝大多数时间，而异常状态发生频率极低，样本的不平衡可能导致异常检测问题的召回率低。

3)缺少标注。时序数据异常检测数据集的标注依赖人工操作，详细标注异常发生的开始和结束时刻。由于专家成本高昂，这类数据集规模通常较小，不能满足一些异常检测算法对训练数据规模的要求。

4)特征工程复杂。软件升级、虚拟机漂移等正常但少数的行为对异常检测提出了挑战。传统的基于阈值的异常检测模型难以准确地识别真正的异常，从而产生许多误报警。

2.4 云平台运维异常

IaaS 云平台的异常可以分为硬件异常和软件异常。根据一些已有的调研工作[10-11]，相比于非云系统，云数据中心运维异常中硬件故障的发生概率较低，软件故障的发生频率有所增加。云平台的硬件包括服务器、存储、网络等设备，大型的云计算中心的硬件设备数量庞大，即使硬件故障发生的概率较低，硬件故障也十分常见。由于云系统的共享性和灵活性，软件错误发生的概率更高，例如不同软件组件或版本的数据格式不一致、因共享资源导致的资源冲突的错误、由于计算机软件或系统的缺陷、故障或者错误，返回了不正确的结果等等。有些软件错误可能会导致程序陷入循环，从而占用大量的计算、内存资源，影响其他程序的正常运行，甚至是虚拟机宕机等。

3　异常检测问题描述

3.1　异常检测模型的数学表达

异常检测问题可以定义为:给定一个数据集 $\boldsymbol{D}$,其中包含大量的正常数据 $\boldsymbol{X}$ 和少量异常数据 $\hat{\boldsymbol{X}}$。异常检测问题是对 $x\in\mathcal{D}$ 预测异常分数 $A(x)$或异常标签 $y(x)\in\{0,1\}$,代表 x 是否为正常数据。

3.2　异常检测的相关技术

3.2.1　异常检测方法的分类

由于在异常检测中难以获取足够的标签数据,半监督的学习方式被广泛使用。在训练阶段,模型对正常数据的特征进行提取和学习,并以此在测试阶段识别数据异常。异常检测的方法可被分为基于预测误差的异常检测和基于重构误差的异常检测。

基于预测的异常检测方法通过使用历史数据预测当前数据来学习样本数据的时序特征。正常数据服从较高的依赖关系,进而能够被相对准确地预测;而异常数据不符合依赖关系,无法进行准确预测。数据的异常分数通过预测数据与实际数据之间的残差计算。

基于重构的异常检测模型利用生成模型将数据映射到潜在特征空间,以对高维复杂数据进行特征提取。正常数据符合数据分布特征,能够被更准确地重构;与之相对,异常数无法被准确重构。数据的异常分数通过重构数据与实际数据之间的残差计算。目前基于深度学习的生成模型有生成式对抗网络(Generative Adversarial Network,GAN)、变分自编码器(Variational Autoencoder,VAE)基于流的生成模型、扩散模型(Diffusion Models)等。其中,扩散模型[12-13]通过逐步向输入数据添加随机噪声直至数据接近随机噪声,再学习逆扩散过程,从噪声中重现原始输入数据,被证明具有更强大的生成性能和稳定性,受到了广泛关注。

不论是基于预测的异常检测方法,还是基于重构的异常检测方法,其异常的判据通常是推断值与实际值之间的残差,或者映射为异常分数。如果残差或分数大于某个阈值,则标注此条数据为异常。因此,自动、动态地为异常检测模型选择合理的阈值,是影响异常检测模型性能的关键因素之一。阈值的选择可以通过最优化异常检测模型的性能指标(F_1 值、F_β 值等)的方式确定,但这种方法需要在验证集中设置系列阈值进行测试,计算量大。一些通过对异常分数的统计分析理论被应用于阈值选择问题中。极值定理(Extreme Value Theory,EVT)是一种不假设数据分布的统计理论,认为极值通常位于概率分布的尾部。峰值过阈值法(Peaks-over-threshold,POT)[14]基于 EVT 理论,用广义帕累托分布拟合数据分布,并识别适当的风险值以动态确定阈值,超过阈值的样本数据为极端数据。

3.2.2　优化算法

随机梯度下降是机器学习中最常用的优化算法,在每次迭代中,随机采样一个样本进行梯度计算。相比于经典梯度算法中采用所有样本的梯度平均进行计算,随机梯度下降显著降低了计算复杂度。此外,由于下降的方向不是全局的下降方向,而是某一个样本的损是函数的下降方向,当某一个函数达到了局部最优后,随着下一次迭代选取了新的目标函数,迭代就可以继续进行。

随机梯度下降算法有较高的学习效率以及一定程度上避免局部最优的能力,但也有着计算需求更高及鞍点的学习能力不足等问题。一些研究对随机梯度下降算法做出了改进,改进重点在于加速收敛过程,尽量避免局部最优,以及减小调参的难度。带动量的随机梯度下降和 Nesterov 动量的随机梯度下降算法模仿了物体运动的惯性,通过积累之前梯度指数级衰减的移动平均,并且继续沿该方向移动,加速了收敛过程。在训练初期,下降方向与之前的方向一致,动量项能够加速下降。在训练中后期,动量项能够增大下降的步伐,跳出局部最小值。在训练的后期,梯度方向发生改变时,动量项将减缓下降,抑制振荡过程。随机梯度下降方法在机器学习中有着广泛的应用,但是在训练过程中选择一个合适的学习率是一件比较困难的事情,往往需要进行大量的实验。而且,在训练过程中,学习率的调整是预先设置好的,无法进行自动调整。为了改进上述问题,一些学者提出了自适应优化器,包括 AdaGrad[15],RMSProp 和 Adam[16] 等。其中,Adam 优化器因超参数具有很好的解释性且通常无需调整或仅需很少的微调,以及在迭代过程中自动调整学习率等诸多优势被广泛应用。

3.2.3　训练数据的预处理

训练数据的预处理一般包括数据清理、数据标准化等过程。数据清理用于判断训练数据中的不规则或错误数据,例如,时序数据的时间戳是否异常,是否有重复、遗漏的数据等。运维数据往往具有不同的量纲和量纲单位,例如 CPU 或内存的利用率取值范围在[0,100],网络连接数则没有一个固定的取值范围,这样的情况会影响到机器学习的效果。原始数据经过数据标准化处理后,各指标处于同一数量级,适合进行综合对比评价。在异常检测问题中,常见的一种数据标准化方法是最大-最小归一化方法:

$$x_i'=\frac{x_i-\min(\boldsymbol{x})}{\max(\boldsymbol{x})-\min(\boldsymbol{x})} \tag{1}$$

3.3　基于深度学习的异常检测学习范式

3.3.1　主动学习

主动学习为减少标注成本提供了一个解决方案,通过选择机器认为难以判断的少量样本进行人工标注,逐步提升模型的效果。主动学习的核心是如何选择需要标注的样本集合,也被称为查询策略。常见的查询策略包括不确定性采样的查询(Uncertainty Sampling)、基于委员会的查询(Query-By-Committee)、基于模型变化期望的查询(Expected Model Change)等[17]。

3.3.2　迁移学习

迁移学习提供了云平台异常检测问题中缺少训练数据的另一个解决方案。一般地,机器学习模型假设训练和测试数据来自相同的特征空间中,具有相同的分布,若分布发生改变,需要从头开始使用新收集的训练数据对模型进行训练。迁移学习基于任务领域之间的知识迁移,适应训练数据和测试数据来自不同的领域、任务和特征空间。因此,针对缺少数据或数据标签的迁移学习模型可利用一个公开的、有标签的数据集进行模型训练,再迁移到目标任务中。迁移学习的另

一个应用场景是在一个新的系统上线初期的异常检测，尚未积累足够的运行数据用于模型训练，利用迁移学习可以在小训练样本上进行快速训练。

迁移学习可以与其他学习范式组合使用，以获得更好的效果。Zhang 等[9]提出了一种主动迁移异常检测方法用于云系统的时序异常检测，结合了主动学习和迁移学习两种技术，如图 2 所示。由现有已标注的数据集对异常检测模型进行训练后，迁移学习将进行从源数据集到目标数据集的知识迁移。由于云服务系统的复杂性，不同系统的时序数据的特征工程也会有很大的差异，主动学习将挑选部分模型数据进行标注以提高模型的性能。实验证明只需要标注 1%～5%的数据即对模型的性能有显著改善。

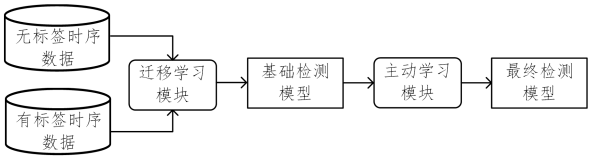

图 2 基于迁移学习的异常检测流程[9]

Fig. 2 Workflow of anomaly detection based on transfer learning[9]

3.3.3 在线学习

在云系统的运行过程中，运行状态随着时间的推移发生变化，时序数据潜在数据分布会随时间发生不可预测的变化，使得原有的模型无法正确地判断数据是否正常，这种现象被称作“概念漂移”。在线学习[18]模型通过历史数据和当前时刻的数据来预测系统当前的状态，并动态调整参数对模型进行更新。

3.3.4 集成学习

由于异常检测问题往往采用无监督或者半监督模型，比有监督学习模型的准确率低。为了改善这类模型的准确率和稳定性，集成学习组合多个模型，不同的学习器之间相互纠正错误，以达到比单一模型更好的性能。集成学习的难点在于如何合并多个模型的结果，传统的集成学习往往采用平均法或者加权平均法，但这意味着得到的结果也是中间的，而非最优的。如图 3 所示，Zhao 等[19]构建了一个 LSCP 框架，对多个异常检测模型进行选择性合并，通过生成伪标签来评估不同异常检测模型在每个测试点生成局部空间的表现，并选择最优的几个模型进行合并，从而提高了异常检测模型的性能。

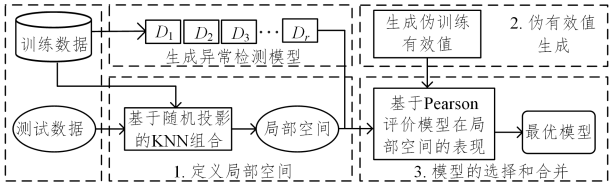

图 3 基于集成学习的异常检测 LSCP 框架[19]

Fig. 3 LSCP frame of anomaly detection based on ensemble learning[19]

3.4 异常检测模型的性能评估

异常检测问题的任务是把数据分为正常或异常，在性能评估中可以用分类问题的相关指标对结果进行评估。对于异常检测的测试数据，记 P 为正常数据的集合，N 为异常数据的集合。对于异常检测的检测结果，记 TP 为真正例的集合，即被正确判定的正常数据；记 TN 为真负例的集合，即被正确判定的异常数据；记 FP 为假正例的集合，即被错误判定的正常数据；记 FN 为假负例的集合，即被错误判定的异常数据。常用的异常检测性能评价指标如表 1 所列。

表 1 异常检测性能评价指标

Table 1 Performance measurement index of anomaly detection

指标名称	计算公式
准确率	$\frac{TP+TN}{P+N}$
错误率	$\frac{FP+FN}{P+N}$
召回率 *recall*)	$\frac{TP}{P}$
精度(*precision*)	$\frac{TN}{N}$
F_1 值(召回率和精度的调和均值)	$\frac{2\times precision\times recall}{precision+recall}$
F_β 值(其中 β 为非负实数)	$\frac{(1+\beta)^2\times precision\times recall}{\beta^2\times(precision+recall)}$

4 面向节点异常检测的时序数据驱动算法

云系统运维异常不一定是某一时刻的数据异常，而是时间维度上的异常，需要对监控数据进行分析判断。针对上述问题，本章总结了时间依赖的运维数据下由时序数据驱动的检测算法。

4.1 节点异常的发现模式

通常，带有时间戳的时序数据 X 可以表示为 $X=[x_1, x_2, x_3, \cdots, x_t]$，其中 x_i 表示时间戳 i($i\in T, T=\{1,2,\cdots,t\}$)的数据。

为了学习到数据中的时间相关性，基于递归的神经网络被学者提出，计算 t 时刻的结果 y_t 时同时考虑当前时刻的输入 x_t 和上一时刻的结果 y_t，可表示为：

$$y_t=f(y_{t-1}, x_t) \tag{2}$$

循环神经网络(Recurrent Neural Networks，RNN)利用神经网络中隐藏层内的反馈回路，将前一时刻的输出作为后续部分神经元的输入信号，从而使神经网络能够捕捉一定时间内不同时刻数据的依赖特征。但应用于云系统的数据规模过大，RNN 的训练十分缓慢，且会出现梯度爆炸或消失的问题。通过改进 RNN 的结构，长短期记忆网络(Long Short-term Memory，LSTM)和门控循环单元网络(Gated Recurrent Units，GRU)被相继提出。LSTM 通过设置输入门、输出门和遗忘门来提高网络对长期数据的记忆能力，同时综合短期记忆计算输出值，解决了 RNN 训练过程中的梯度问题，对数据在时间维度上的依赖关系有着更强的捕捉能力。GRU 是 LSTM 的简化版，用一个门来同时控制输入和输出，提高了训练的速度，但同样有很好的训练效果。

Malhotra 等[20]将基于预测误差的 LSTM 神经网络应用到了时序数据的异常检测中。相较于一般的异常检测模型，LSTM 有着优秀的长期记忆能力，在训练和测试中不需要预先指定时间窗口即可检测出数据的行为偏差。通过堆叠 LSTM 增加了网络的层数，模型能够学习到更高水平的时序特征。在训练过程中，使用非异常的数据模型并将预测误差建模为高斯分布，用于评估异常行为。Li 等[21]提出了基于重构误差的多变量时间序列异常检测模型 MAD-GAN，将 LSTM 和 RNN 嵌入 GAN 中捕捉数据时间上的依赖关系，同

时利用生成器的重建误差和判别器的判别误差检测异常数据。Su 等[22]提出用于多变量时间序列异常检测的随机递归神经网络 OmniAnomaly 模型，并基于 VAE 的重构误差判断异常。

由于递归神经网络无法并行的问题，模型的计算速度无法满足运维场景下的要求，Bai 等[23]提出了时域卷积网络（Temporal Convolutional Network，TCN），可表示为：

$$y_t = f(x_0, x_1, \cdots, x_t) \tag{3}$$

如图 4 所示，TCN 利用卷积对时序数据提取序列数据的时间特性，利用因果卷积对时序数据进行预测，利用扩张卷积对时序数据进行间隔采样，以在同等深度的网络中获得更大的感受野。随着时序数据窗口的增大，扩张卷积的层数增加，TCN 网络的深度不断加深，为了避免梯度消失的问题，TCN 构建了残差连接。卷积网络很好地改善了递归网络中无法并行的问题，极大地提高了计算速度，且更容易捕捉到全局的信息。

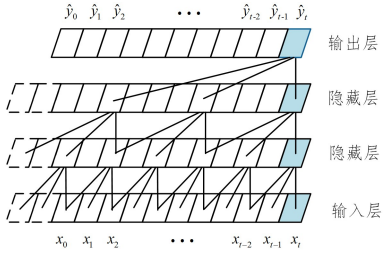

图 4　扩张因果卷积结构[23]

Fig. 4　Structure of dilated causal convolution[23]

He 等[24]提出了一种基于预测误差的 TCN 神经网络用于时序数据的异常检测，在训练过程中利用 TCN 对正常数据进行特征提取，在预测模型中使用了多层特征提取合并的结构以获得更好的预测效果。TCN-AE[25]构建了一个基于自编码结构的时域卷积网络来识别具有周期性的复杂网络时序异常，基于焦点得分的自我调节来实现鲁棒的多模态特征提取和对抗训练，以获得稳定性。由于自编码器无法处理数据的随机性，基于 VAE 结构的 MST-VAE 模型[26]被提出，并结合短尺度和长尺度的卷积核来提取时间序列的不同尺度的时间信息以提升模型性能。

谷歌机器翻译团队提出的依靠注意力机制捕捉序列关联的 Transformer 模型[27]将注意力机制引入时序数据。该模型没有使用递归和卷积的结构，依靠编码器-解码器架构和注意力机制处理序列数据，有着并行计算、计算复杂度更低、可解释性更强等优势。在此基础上，Xu 等[28]将 Transformer 模型应用于异常检测领域，提出了 Anomaly Transformer 模型。该模型基于注意力机制学习时间序列中每一个点与整个序列的关联表示，相比于正常点来说，异常点很难与序列的所有点都构建很强的关联，且由于连续性，异常节点和其邻近区域往往有很强的关联性。这种整个序列和邻近先验之间的关联差异为时序异常检测提供了有力的判据。Anomaly Transformer 模型包含用于建模先验关联和时序关联的 Anomaly-Attention，并基于重构误差和极小极大策略的关联差异来区分正常点和异常点。TranAD[29]是一个基于深度 Transformer 网络的模型，利用基于注意力的序列编码来在更广的时间窗口做出快速的推理。本文中提到的部分时序数据驱动的异常检测算法如表 2 所列。

表 2　数据驱动的异常检测算法总结

Table 2　Summary of data-driven anomaly detection algorithms

	基于预测误差	基于重构误差
递归网络	[20]	[21-22]
时域卷积网络	[24]	[25-26]
Transformer 网络	[29]	[28]

4.2　流数据场景下的在线检测

在云运维过程中，每一组云监控系统的数据按照时间顺序依次到达，异常检测模块需要实时给出推断结果。在线异常检测面临一些挑战：一是在云系统的运行过程中，软件的升级、虚拟机的漂移等行为时常发生，改变了系统的运行状态，称之为流数据的概念漂移；二是在线异常检测模型需要提前预知到故障，而不仅是感知到已经发生的故障，因为故障的发生往往意味着严重的后果。Ahmad 等[30]提出基于分层时间记忆网络（Hierarchical Temporal Memeory，HTM），构建了一个在线学习高效地处理流数据的异常检测方法，对数据的变化进行持续的适应和调整，能够尽早推测异常的发生。

5　面向网络异常发现的图数据驱动算法

IaaS 云平台是一个基于网络的资源池，云平台中的节点都通过网络与其他节点存在联系，而非孤立存在。例如，部分虚拟机共同部署在同一个宿主机上，部分设备通过负载均衡共同承担某项任务，某个业务系统的数据库服务器和系统服务器存在大量的互访关系等等。时序性能指标在节点层面描述节点的运行状态，但无法体现节点与节点之间的关联性。因此一些研究将云系统的拓扑信息引入到异常检测算法中，系统的拓扑信息和时序性能指标共同构成了系统级别的信息。

5.1　图数据结构

云系统的拓扑信息可以用图数据结构进行建模。图由两个集合构成，一个是非空但有限的顶点的集合 $\boldsymbol{V}$，另一个是边的集合 $\boldsymbol{E}$，每条边对应一对顶点 (v, w)，其中 $v, w \in \boldsymbol{V}$，一个图数据被表示为 $\boldsymbol{G} = \{\boldsymbol{V}, \boldsymbol{E}\}$。

为云系统监控的时空数据构建数学模型，主要的方法分为两种：一是基于系统设备之间的关联性建立[31]，定义系统中的每一个设备为一个节点，将互相通信的设备之间定义为图的边；二是基于图结构的学习建立[32]，定义每个性能指标为节点，通过计算指标间的相关性对图结构进行学习，定义相关性较高的节点之间存在有向边，进而进行网络异常发现。

5.2　图神经网络

图数据是一种复杂的数据结构，对其进行处理也比较困难。图神经网络（Graph Neural Networks，GNN）[33]是处理图数据问题在深度学习上的一个重要模型。GNN 模型中假定每个节点由自身和所有邻居节点的特征信息共同定义，训练过程对每个节点的自身和所有邻居节点进行加权求和，来更新节点 v 的隐藏状态 h_v，随着 GNN 层数的增加，h_v 将不断包含网络中更多节点的节点特征。为了提取到数据的更高级特征，Kipf 等[34]基于卷积理论提出了图卷积神经网络（Graph Convolution Networks，GCN）。与 GNN 相比，GCN 主要优化了加权求和中的权重问题，通过卷积算子提取节点自身和所有邻居节点的特征信息。但是，GCN 无法为不同邻居节点的特征赋予不同的权重，这限制了其提取空间信息的能力；且提取邻近节点特征的方式取决于图的结构，局限了其在其他图

上的泛化能力。为了弥补 GCN 在上述方面的局限性，Velikovi[35]将注意力机制引入了图神经网络，提出了图注意力网络(Graph Attention Network，GAT)，通过注意力机制提取节点自身和所有邻居节点的特征信息，权重的选取完全取决于节点特征，与图结构无关。

5.3 网络异常模式的发现

为了同时学习数据的时间和空间特征，一种思路是将图神经网络模块和时序数据处理模型结合。He 等[31]构建了 GraphLSTM 模块，将图神经网络和 LSTM 连接，用图神经层替换掉 LSTM 中的全连接层，进而基于 VAE 的重构误差构建拓扑感知的多元时序数据异常检测模型，其结构如图 5 所示。AddGraph 模型[36]定义每个时间戳下的图数据为一个快照，利用基于注意力机制的 GRU 扩展了 GCN 模型，使得 GCN 在处理图结构的同时考虑到图中节点的时序因素。STA-GAN 模型[37]基于时序注意力机制和空间注意力机制构建了时空注意力模块，分别学习数据的短期时序相关性和动态空间依赖关系。

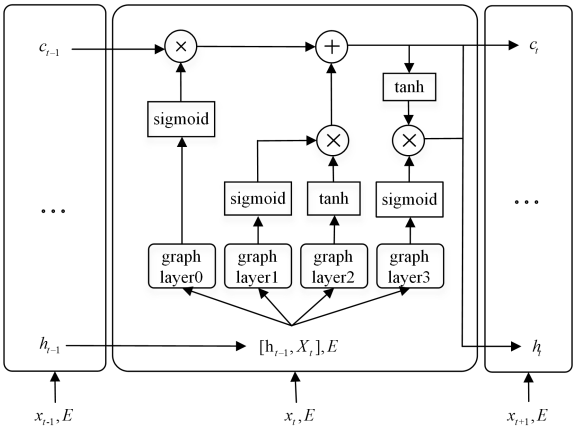

图 5 GraphLSTM 结构[31]

Fig. 5 Structure of GraphLSTM[31]

由于图数据的复杂性，其异常检测往往需要庞大的计算，具有很大的挑战性。因此一些文章引入了图嵌入技术，将高维图数据表示成向量，同时保留网络的拓扑结构和节点信息，进而能够适用于更多的机器学习算法。NetWalk[38]将图嵌入技术引入了动态图结构中，通过学习网络结构信息以检测动态图数据中的异常节点，通过自编码器学习节点的初始表示并根据网络的发展添加或删除节点，基于聚类的方法动态、增量地进行异常检测。由于图结构的复杂性，图数据的异常检测问题依然存在挑战[39]：不同时间戳间时间维度和空间维度的信息提取问题；节点、边、子图和图变化趋势的发现问题等。

6 数据驱动下 IaaS 云运维数据异常检测中的新问题与新挑战

随着数据驱动的异常检测模型的发展，异常检测模型的性能也在不断提高，同时也带来了新的问题与挑战，包括数据的标注以及模型的计算效率等方面。

6.1 如何减少数据标注成本

如前文所述，为训练数据进行标注是一项昂贵且耗时的工作，数据标注的工作量是大规模数据集异常检测工作最主要的难点。为了减轻添加数据标签的工作量，Zhao 等[40]设计了一种基于异常相似搜索的半自动化标注工具，利用孤立森林进行无监督的异常检测，筛选出候选异常，专家对某一异常进行标注后，工具将自动匹配相似的异常，减少专家标注时间。此外，迁移学习和主动学习技术的应用也降低了数据标注的要求。Zhang 等[41]提出一种主动迁移异常检测模型实现跨数据集的异常检测，只需标记 1%～5%的目标集未标记数据。

6.2 如何处理数据标签的污染

在解决现实问题中，训练数据集的数据标签可能与它们真实的情况不相符，称之为数据标签的污染。由于数据的标签是人工添加的，标签存在错误是有可能会发生的。而且，很多情况下，对数据添加标签的任务是具有主观性的，位于边界的数据点可能会被错误标记。数据标签的污染会削弱机器学习模型的性能。很多学者针对这个问题展开了研究。Verleysen 等[42]总结了 3 类对抗数据标签污染的方法：1)一些模型的结构有天然的鲁棒属性，对标签污染的敏感度低；2)在数据清理阶段，对有标签进行过滤和处理，订正或是删除标签有误的数据；3)一些算法在学习过程中对标签噪声进行建模，或将已有的模型嵌入标签污染的模型，这类方法能将模型和标签噪声模型分开，从而允许使用有关标签噪声性质的信息。

6.3 如何满足流数据场景下的计算效率要求

在流数据场景下，异常检测的计算效率是一个重要的因素。如果不能及时地给出异常检测的结果，运维人员则无法及时地处理故障。如何轻量化异常检测模型，快速判断系统运行状态，是研究的方向之一。SCWarn 模型[43]是一种有着轻量且高效网络结构的异常检测模型，训练时长只有几分钟，检测时常小于 1s，较其他模型有极大改善。

结束语 随着云计算规模和复杂性不断扩大，用户对系统的要求不断提升，系统的运维工作问题面临越来越多的挑战。基于深度学习等人工智能技术，自动从海量监测数据中总结规律，并做出决策的智能化运维是未来的发展方向。本文从面向 IaaS 云计算节点的异常检测和面向 IaaS 云计算平台的系统级异常检测总结了近年来异常检测的新方法、新技术，并分析了现阶段云运维出现的新问题和新挑战。随着人工智能和深度学习相关技术的发展，云运维异常检测算法将愈加完善，为 IaaS 云的智能运维提供坚实支撑。

参 考 文 献

[1] JIANG P. Development and Application of Smart Ocean Cloud Platform under the Internet of Things[J]. Journal of Marine Information Technology and Application, 2022, 3: 10-17.

[2] SUN C, WANG Y, PAN Z, et al. Design and implementation of island information management and display system based on cloud storage technology[J]. Marine Science Bulletin, 2019, 2: 233-240.

[3] QIU J, DU Q, QIAN C. KPI-TSAD: A Time-Series Anomaly Detector for KPI Monitoring in Cloud Applications[J]. Symmetry, 2019, 11: 1350.

[4] GUERRON X, ABRAHO S, INSFRAN E, et al. A taxonomy of quality metrics for cloud services[J]. IEEE Access, 2020, 8: 131461-131498.

[5] MENG W, LIU Y, ZHU Y, et al. LogAnomaly: Unsupervised Detection of Sequential and Quantitative Anomalies in Unstructured Logs[C]// Twenty-Eighth International Joint Conference

on Artificial Intelligence(IJCAI-19). 2019:4739-4745.

[6] XIU Z. Request Tracing and Anomalies Detecting System in Cloud[D]. Wuhan: Huazhong University of Science and Technology, 2014.

[7] LAVIN A, AHMAD S. Evaluating Real-Time Anomaly Detection Algorithms — The Numenta Anomaly Benchmark[C]// IEEE 14th International Conference on Machine Learning and Applications(ICMLA). 2015:38-44.

[8] LI Z Y, ZHAO N W, ZHANG S L, et al. Constructing Large-Scale Real-World Benchmark Datasets for AIOps [J/OL]. (2022-08-08)[2023-03-08]. https://doi. org/10. 48550/arXiv. 2208. 03938.

[9] ZHANG X, LIN Q, XU Y, et al. Cross-dataset time series anomaly detection for cloud systems[C]// USENIX Annual Technical Conference. USENIX Association, 2019:1063-1076.

[10] LIU H, LU S, MUSUVATHI M, et al. What bugs cause production cloud incidents?[C]// Proceedings of the Workshop on Hot Topics in Operating System. ACM, 2019:155-162.

[11] VISHWANATH K V, NAGAPPAN N. Characterizing Cloud Computing Hardware Reliability[C]// Proceedings of the 1st ACM Symposium on Cloud Computing. ACM, 2010:193-204.

[12] SOHL-DICKSTEIN J, WEISS E A, MAHESWARANATHAN N, et al. Deep Unsupervised Learning Thermodynamics[C]// Proceedings of the 32nd International Conference on International Conference on Machine Learning. ACM, 2015:2256-2265.

[13] HO J, JAIN A, ABBEEL P. Denoising Diffusion Probabilistic Models[J/OL]. (2020-12-16)[2023-03-08]. https://arxiv. org/abs/2006. 11239.

[14] SIFFER A, FOUQUE P A, TERMIER A, et al. Anomaly Detection in Streams with Extreme Value Theory[C]// Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. ACM, 2017:1067-1075.

[15] WARD R A, WU X, BOTTOU L. AdaGrad stepsizes: sharp convergence over nonconvex landscapes[C]// Proceedings of the 36th International Conference on Machine Learning. 2019:6677-6686.

[16] KINGMA D, BA J. Adam: A Method for Stochastic Optimization[J/OL]. (2017-01-30)[2023-03-08] https://doi. org/10. 48550/arXiv. 1412. 6980.

[17] SETTLES B. Active Learning Literature Survey[J/OL]. (2012-03-15)[2023-04-01]. http://digital. library. wisc. edu/1793/60660.

[18] HAN S, WU Q, ZHANG H, et al. Log-based Anomaly Detection with Robust Feature Extraction and Online Learning[J]. IEEE Transactions on Information Forensics and Security, 2021, 16:2300-2311.

[19] ZHAO Y, NASRULLAH Z, HRYNIEWICKI M K, et al. LSCP: Locally Selective Combination in Parallel Outlier Ensembles[C]// Proceedings of the 2019 SIAM International Conference on Data Mining. 2019:585-593.

[20] MALHOTRA P, VIG L, SHROFF G, et al. Long Short Term Memory Networks for Anomaly Detection in Time Series[C]// 23rd European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning. 2015.

[21] LI D, CHEN D, SHI L, et al. MAD-GAN: Multivariate Anomaly Detection for Time Series Data with Generative Adversarial Networks[C]// Artificial Neural Networks and Machine Learning(ICANN 2019): Text and Time Series: 28th International Conference on Artificial Neural Networks. ACM, 2019: 703-716.

[22] SU Y, ZHAO Y, NIU C, et al. Robust Anomaly Detection for Multivariate Time Series through Stochastic Recurrent Neural Network[C]// Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining. 2019:2828-2837.

[23] BAI S J, ZICO K J, KOLTUN V, et al. An Empirical Evaluation of Generic Convolutional and Recurrent Networks for Sequence Modeling[J/OL]. (2018-04-19)[2023-04-08]. https://doi. org/10. 48550/arXiv. 1803. 01271.

[24] HE Y, ZHAO J. Temporal Convolutional Networks for Anomaly Detection in Time Series[J]. Journal of Physics: Conference Series, 2019, 1213:042050.

[25] THILL M, KONEN W, WANG H, et al. Temporal convolutional autoencoder for unsupervised anomaly detection in time series[J]. Applied Soft Computing, 2021, 3:107751.

[26] PHAM T, LEE J, PARK C. MST-VAE: Multi-Scale Temporal Variational Autoencoder for Anomaly Detection in Multivariate Time Series[J]. Applied Sciences, 2022, 12(19):10078.

[27] VASWANI A, SHAZEER N, PARMAR N, et al. Attention Is All You Need[J/OL]. (2017-12-06) [2023-03-08]. https://doi. org/10. 48550/arXiv. 1706. 03762.

[28] XU J, WU H, WANG J, et al. Anomaly Transformer: Time Series Anomaly Detection with Association Discrepancy [J/OL]. (2022-06-29) [2023-03-08]. https://doi. org/10. 48550/arXiv. 2110. 02642.

[29] TULI S, CASALE G, JENNINGS N R. TranAD: Deep Transformer Networks for Anomaly Detection in Multivariate Time Series Data[J]. Pro. VLDB Endow, 2022, 15:1201-1214.

[30] AHMAD S, LAVIN A, PURDY S, et al. Unsupervised real-time anomaly detection for streaming data [J]. Neurocomputing, 2017, 262:134-147.

[31] HE Z, CHEN P, LI X, et al. A Spatiotemporal Deep Learning Approach for Unsupervised Anomaly Detection in Cloud Systems[J]. IEEE Transactions on Neural Networks and Learning Systems, 2023, 34(4):1705-1719.

[32] DENG A, HOOI B. Graph Neural Network-Based Anomaly Detection in Multivariate Time Series [C]// Proceedings of the AAAI Conference on Artificial Intelligence, 2021, 35(5):4027-4035.

[33] SCARSELLI F, GORI M, TSOIA C, et al. The Graph Neural Network Model[J]. IEEE Transactions on Neural Networks, 2009, 20(1):61-80.

[34] KIPF T, WELLING M. Semi-Supervised Classification with Graph Convolutional Networks[J/OL]. (2017-02-22)[2023-03-08]. https://doi. org/10. 48550/arXiv. 1609. 02907 907K.

[35] VELIKOVI P, CUCURULL G, CASANOVA A, et al. Graph Attention Networks[J/OL]. (2018-02-04) [2023-03-08]. ht-

tps://doi.org/10.48550/arXiv.1710.10903.

[36] ZHENG L, LI Z, LI J, et al. AddGraph: Anomaly Detection in Dynamic Graph Using Attention-based Temporal GCN[C]// Twenty-Eighth International Joint Conference on Artificial Intelligence(IJCAI-19). 2019: 4419-4425.

[37] WANG S, LI W, HOU S, et al. STA-GAN: A Spatio-Temporal Attention Generative Adversarial Network for Missing Value Imputation in Satellite Data[J]. Remote Sensing, 2022, 15: 88.

[38] YU W, WEI C, AGGARWAL C C, et al. NetWalk: A Flexible Deep Embedding Approach for Anomaly Detection in Dynamic Networks[C]// The 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining. 2018: 2672-2681.

[39] MA X, WU J, XUE S, et al. A Comprehensive Survey on Graph Anomaly Detection with Deep Learning[J]. IEEE Transactions on Knowledge and Data Engineering, 2023, 35(12): 12012-12038.

[40] ZHAO N, ZHU J, LIU R, et al. Label-Less: A Semi-Automatic Labelling Tool for KPI Anomalies[C]// IEEE Conference on Computer Communications (INFOCOM 2019). IEEE, 2019: 1882-1890.

[41] ZHANG X, LIN Q, XU Y, et al. Cross-dataset Time Series Anomaly Detection for Cloud Systems[C]// USENIX Annual Technical Conference. 2019: 1063-1076.

[42] VERLEYSEN M, FRENA Y. Classification in the Presence of Label Noise: A Survey[J]. IEEE Transactions on Neural Networks and Learning Systems, 2014, 25(5): 845-869.

[43] ZHAO N, CHEN J, YU Z, et al. Identifying bad software changes via multimodal anomaly detection for online service systems [C]// Proceedings of the 29th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering. 2021: 527-539.

SI Jia, born in 1994, postgraduate, assistant engineer. Her main research interests include marine information system and so on.

DENG Yingjun, born in 1986, Ph.D, lecturer. His main research interests include predictive maintenance and machine learning.